

# Properties of element orders in covers for $L_n(q)$ and $U_n(q)$

ANDREI V. ZAVARNITSINE<sup>1</sup>

Sobolev Institute of Mathematics,  
pr. Koptyuga 4, Novosibirsk, 630090, Russia

UDC 512.54

## Abstract

We show that if a finite simple group  $G$  isomorphic to  $PSL_n(q)$  or  $PSU_n(q)$ , where either  $n \neq 4$ , or  $q$  is prime or even, acts on a vector space over a field of the defining characteristic of  $G$ , then the corresponding semidirect product contains an element whose order is distinct from every element order of  $G$ . As a consequence, we prove that the group  $PSL_n(q)$ ,  $n \neq 4$  or  $q$  prime or even, is recognizable by spectrum from its covers thus giving a partial positive answer to Problem 14.60 from the Kourovka notebook.

## 1 Introduction

If a group  $H$  is a homomorphic image of a finite group  $G$  then we say that  $G$  is a *cover* for  $H$ , or that  $G$  *covers*  $H$ . This paper is devoted to the following problem included in the Kourovka notebook [1, Problem 14.60]:

**Problem 1** *Suppose that  $G$  is a proper cover for the finite simple group  $L = L_n(q)$ ,  $n \geq 3$ . Is it true that  $G$  contains an element whose order is distinct from the order of every element of  $L$ ?*

This problem is related to the recognition of finite groups by spectrum. Recall that the *spectrum*  $\omega(H)$  of a finite group  $H$  is the set of its elements orders. We call  $H$  *recognizable (by spectrum) from its covers* if, for every finite group  $G$  covering  $H$ , the equality of the spectra  $\omega(G) = \omega(H)$  implies the isomorphism  $G \cong H$ . Thus, Problem 1 asks if every simple group  $L_n(q)$ ,  $n \geq 3$ , is recognizable from its covers.

Some special cases of this problem have already been treated elsewhere, e. g. [2, 3, 4]. Moreover, the simple groups  $L_2(q)$  are recognizable from their covers due to [5, 6].

It can be shown (see Lemma 12) that the consideration of Problem 1 may be reduced to the case where the cover  $G$  is the natural semidirect product  $W \rtimes L$ , where  $W$  is an elementary abelian  $p$ -group,  $p$  being the defining characteristic for  $L = L_n(q)$ , and the action of  $L$  on  $W$  is faithful and absolutely irreducible. We prove that such a  $G$  usually contains an element of new order. More precisely, if we denote  $L_n^+(q) = PSL_n(q)$  and  $L_n^-(q) = PSU_n(q)$ , then the following holds:

**Theorem 1** *Let  $\varepsilon \in \{+, -\}$  and let  $L = L_n^\varepsilon(q)$ ,  $q = p^m$  be a simple group. Suppose that either  $n \geq 5$ , or  $n = 4$  and  $q$  is prime, or  $n = 4$  and  $q$  is even. If  $L$  acts on a vector space  $W$  over a field of characteristic  $p$  then  $\omega(W \rtimes L) \neq \omega(L)$ .*

As follows from the proof, in the case where either  $n \geq 5$  or  $q$  is an odd prime we can assert even more: the group  $L$  contains a *semisimple* element  $g$  of  $p$ -maximal order (i.e. such that  $p \nmid |g| \notin \omega(L)$ ) which centralizes a nontrivial vector in  $W$ . Moreover, if  $n \geq 5$  and  $q > 3$ , such an

<sup>1</sup>supported by FAPESP, Brazil, Proc. 06/60766-3; RFBR, Russia, grant 05-01-00797; SB RAS, grant No.29 for young scientists and Integration Project 2006.1.2

element  $g$  may be chosen independent of the module  $W$ . The proof uses the properties of weights of the irreducible modules for the algebraic group of type  $A_l$ .

As a consequence of this result, we have the following (partial) affirmative solution to Problem 1:

**Corollary 1** *Let  $L = L_n(q)$  be a simple linear group. If either  $n \neq 4$ , or  $q$  is prime, or  $q$  is even then  $L$  is recognizable by spectrum from its covers.*

Therefore, the only remaining unresolved case for Problem 1 is where  $L = L_4(q)$  with  $q$  odd and nonprime. We observe that the action of  $L_4^\varepsilon(q)$  in the defining characteristic turned out to be a more subtle issue. The above methods will not always work as there are examples of semidirect products  $W \rtimes L$  which do not contain elements of order  $pt$  for  $p$ -maximal order  $t$  coprime with  $p$ . This means that the action of unipotent elements of  $L_4^\varepsilon(q)$  should also be taken account of. For example, in characteristic  $p = 2$ , let  $W$  be the natural module for  $L = \mathrm{SU}_4(2)$ . Then  $\omega(W \rtimes L) \setminus \omega(L) = \{8\}$ . There are also more complicated examples of this kind in odd characteristic.

## 2 Preliminaries

In what follows, we denote by  $\mathbb{F}_q$  a finite field of  $q = p^m$  elements. The center of a group  $G$  is  $Z(G)$ .

Let  $t > 1$  and  $n$  be natural numbers and let  $\varepsilon \in \{+, -\}$ . If there exists a prime that divides  $t^n - (\varepsilon 1)^n$  and does not divide  $t^i - (\varepsilon 1)^i$  for  $1 \leq i < n$ , then we denote this prime by  $t_{[\varepsilon n]}$  and call it a *primitive divisor* of  $t^n - (\varepsilon 1)^n$ . In general, a primitive divisor need neither exist nor be unique. The following lemma is a generalization of the well-known Zsigmondy's theorem:

**Lemma 2** *Let  $t, n > 1$  be natural numbers and  $\varepsilon \in \{+, -\}$ . There exists a primitive divisor  $t_{[\varepsilon n]}$  of  $t^n - (\varepsilon 1)^n$ , except in the following cases:*

- (i)  $\varepsilon = +, n = 6, t = 2$ ;
- (ii)  $\varepsilon = +, n = 2$ , and  $t = 2^l - 1$  for some  $l \geq 2$ ;
- (iii)  $\varepsilon = -, n = 3, t = 2$ ;
- (iv)  $\varepsilon = -, n = 2$ , and  $t = 2^l + 1$  for some  $l \geq 0$ .

*Proof.* See [4, Lemma 5].  $\blacktriangle$

Let  $q$  be a power of a prime and let  $\varepsilon \in \{+, -\}$ . For  $n \in \mathbb{N}$ , we define the *generalized primitive divisor*

$$q_{[\varepsilon n]}^* = \begin{cases} q_{[\varepsilon n]}, & \text{if } q_{[\varepsilon n]} \text{ exists,} \\ 9, & \text{if } (\varepsilon, n, q) = (+, 6, 2), \\ 2^l, & \text{if } (\varepsilon, n, q) = (+, 2, 2^l - 1) \text{ for } l \geq 2, \\ 2^l, & \text{if } (\varepsilon, n, q) = (-, 2, 2^l + 1) \text{ for } l \geq 2. \end{cases}$$

Observe that  $q_{[\varepsilon n]}^*$  is not defined if and only if

$$(\varepsilon, n, q) \in \{(-, 2, 2), (-, 2, 3), (-, 3, 2)\}. \quad (1)$$

The following assertion follows directly from the above definition:

**Lemma 3** *Suppose that  $r = q_{[\varepsilon n]}^*$  is defined. Then*

- (i)  $r \mid (q^s - (\varepsilon 1)^s)$  if and only if  $n \mid s$ ;
- (ii) for  $n > 1$ , we have  $\gcd(r, q - \varepsilon 1) = 1$ , unless  $(\varepsilon, n, q) = (+, 2, 2^l - 1)$  or  $(-, 2, 2^l + 1)$ ;
- (iii) if  $s \mid n$  and  $s > 1$  then

$$r \mid \frac{q^n - (\varepsilon 1)^n}{q^{n/s} - (\varepsilon 1)^{n/s}}, \quad (2)$$

unless  $(\varepsilon, n, s, q) = (+, 6, 3, 2)$ ;

- (iv) for  $n > 1$ , the group  $\mathrm{SL}_n^\varepsilon(q)$  contains an irreducible element of order  $r$ .

In the following lemmas, a quotient of the finite group  $\mathrm{SL}_n^\varepsilon(q)$  by a central subgroup is said to be a group of type  $A_{n-1}^\varepsilon(q)$ .

**Lemma 4** *Let  $q$  be a power of a prime  $p$ . A group of type  $A_{n-1}^\varepsilon(q)$  contains an element of order  $p^{t+1}$ ,  $t \geq 0$ , if and only if  $n \geq p^t + 1$ .*

*Proof.* See [8, Corollary 0.5]  $\blacktriangle$

**Lemma 5** (i) *Let  $L = \mathrm{L}_n^\varepsilon(q)$  be a simple group. Then the numbers*

$$\frac{q^n - (\varepsilon 1)^n}{d(q - \varepsilon 1)}, \quad \frac{q^{n-1} - (\varepsilon 1)^{n-1}}{d} \quad (3)$$

*are coprime and maximal by divisibility elements of  $\omega(L)$ .*

(ii) *Let  $n \in \mathbb{N}$ , let  $q$  be a power of a prime  $p$  and let  $\varepsilon \in \{+, -\}$ . Suppose that  $n = s + b_1 + \dots + b_k$ , where  $s = 0$  or  $s = p^t$  with  $t \geq 0$ ,  $k \geq 0$ , and all  $b_i$ 's are pairwise coprime and greater than 1. If  $(\varepsilon, q) = (-, 2)$  then we assume additionally that  $b_i \neq 2, 3$  for all  $i$ . If  $(\varepsilon, q) = (-, 3)$  then we assume that  $b_i \neq 2$  for all  $i$ . Put  $r_i = q_{[\varepsilon b_i]}^*$  (which exists due to the restrictions on  $b_i$ ). Then  $p^{t+1}r_1 \cdot \dots \cdot r_k \notin \omega(\mathrm{SL}_n^\varepsilon(q))$ , where it is assumed that  $t = 0$  if  $s = 0$ .*

*Proof.* We prove item (ii) first. The particular case  $s = p^t$  was proved in [4, Lemma 9]; however, we do not exclude it from the consideration as we give here a different proof. Suppose to the contrary that there is  $a \in \mathrm{SL}_n^\varepsilon(q)$  of order  $p^{t+1}r_1 \cdot \dots \cdot r_k$ . Then  $a$  lies in the centralizer  $C$  in  $\mathrm{SL}_n^\varepsilon(q)$  of the semisimple element  $u = a^{p^{t+1}}$ . By [7, Propositions 7, 8],  $C$  is a central product of groups  $M_{i,j}$ ,  $i \geq 2$ , of type  $A_{i-1}^\varepsilon(q^{\mu_j^{(i)}})$  extended by an abelian group  $T$  of order  $\prod_{i,j} (q^{\mu_j^{(i)}} - (\varepsilon 1)^{\mu_j^{(i)}}) / (q - \varepsilon 1)$ , where  $\mu^{(i)}$  is a partition of  $n_i$  and the numbers  $n_i$  satisfy  $\sum i n_i = n$ . In particular,

$$\sum_{i,j} i \mu_j^{(i)} = n. \quad (4)$$

Observe that  $u \in Z(C)$  and  $Z(C)$  is an abelian group of order dividing  $\prod_{i,j} (q^{\mu_j^{(i)}} - (\varepsilon 1)^{\mu_j^{(i)}})$ . Since  $|u| = r_1 \cdot \dots \cdot r_k$ , by Lemma 3(i) it follows that, for each  $f = 1, \dots, k$ , there are  $i, j$  such that  $b_f$  divides  $\mu_j^{(i)}$  (if  $r_f$  is not prime then we should also recall that  $Z(C)$  is in fact a subgroup of the direct product of cyclic groups of the orders  $q^{\mu_j^{(i)}} - (\varepsilon 1)^{\mu_j^{(i)}}$  for all  $i, j$ ). By hypothesis, all the numbers  $b_f$  are coprime and greater than 1; hence, the sum of those  $\mu_j^{(i)}$  greater than 1 is at least  $b_1 + \dots + b_k$ .

Now, because  $C$  contains an element of order  $p^{t+1}$ , one of the above components  $M_{i',j'}$  is nontrivial and such that  $i' \geq p^t + 1$  by Lemma 4. If  $\mu_{j'}^{(i')} = 1$ , we have

$$\sum_{i,j} i \mu_j^{(i)} \geq b_1 + \dots + b_k + p^t + 1 > n, \quad (5)$$

contrary to (4). If  $\mu^{(i')}_{j'} > 1$ , then  $i' \mu^{(i')}_{j'} \geq p^t + 1 + \mu^{(i')}_{j'}$ , and we still have (5). This contradiction completes the proof.

We now prove (i). First, following the above argument we show that the numbers in (3) are in  $\mu(M)$ . Let  $k$  denote either of these numbers. It is well-known that  $L$  contains an element of order  $k$ . We show the maximality of  $k$  in  $\omega(L)$  (with respect to divisibility). We may assume that  $(\varepsilon, n, q) \neq (-, 3, 3), (-, 4, 2)$ , because, for the groups  $U_3(3)$  and  $U_4(2)$ , the assertion is readily verified. Suppose that there is an element  $\bar{a} \in L$  of order a multiple of  $k$ . Then the preimage  $a \in S = \text{SL}_n^\varepsilon(q)$  of  $\bar{a}$  lies in the centralizer  $C$  in  $S$  of a semisimple element  $u$  of order  $k$ . Observe that the generalized primitive divisor  $r = q_{[\varepsilon n]}^*$  (respectively,  $r = q_{[\varepsilon(n-1)]}^*$ ) exists, since  $L \neq U_3(3), U_4(2)$ . Then  $u \in Z(C)$  and we conclude as above that  $n$  (respectively,  $n-1$ ) divides some  $\mu^{(i)}_j$ . But then (4) implies that the decomposition for  $n$  is  $n = n_1 = \mu^{(1)}_1$  (respectively,  $n = n_1 = \mu^{(1)}_1 + \mu^{(1)}_2$ , where  $\mu^{(1)}_1 = n-1$  and  $\mu^{(1)}_2 = 1$ ). In particular,  $C$  coincides with its toral part  $T$  isomorphic to the cyclic group of order  $(q^n - (\varepsilon 1)^n)/(q - \varepsilon 1)$  (respectively,  $q^{n-1} - (\varepsilon 1)^{n-1}$ ). Due to the conjugacy of the maximal tori,  $T$  contains the center  $Z(S)$  of order  $d$  and hence the order of  $\bar{a} \in T/Z(S)$  does not exceed  $k$ .

We finally show that the numbers in (3) are coprime. Denote

$$x = \frac{(\varepsilon q)^n - 1}{\varepsilon q - 1}, \quad y = \frac{\varepsilon q - 1}{d}, \quad z = \frac{(\varepsilon q)^{n-1} - 1}{\varepsilon q - 1}.$$

Then up to sign the numbers in (3) coincide with  $x/d$  and  $yz$ , respectively. Note that  $\gcd(x, z) = 1$ , since

$$\gcd((\varepsilon q)^n - 1, (\varepsilon q)^{n-1} - 1) = (\varepsilon q)^{\gcd(n, n-1)} - 1 = \varepsilon q - 1.$$

Also, setting  $f(t) = t^{n-1} + \dots + t + 1 \in \mathbb{Z}[t]$  we can find  $g(t) \in \mathbb{Z}[t]$  such that  $f(t) = (t-1)g(t) + n$ . Then the substitution  $t = \varepsilon q$  gives  $x = f(\varepsilon q) \equiv n \pmod{\varepsilon q - 1}$ . Thus,  $\gcd(x, \varepsilon q - 1) = \gcd(n, \varepsilon q - 1) = d$  and so  $\gcd(x/d, y) = 1$ . The claim follows from these remarks.  $\blacktriangle$

**Lemma 6** (i) *For every real  $x \geq 22$ , the interval  $(x/3, x/2]$  contains at least one prime.*

(ii) *For every real  $x \geq 57$ , the interval  $(2x/3, x - 16]$  contains at least one prime.*

(iii) *For every real  $x > 45$ , the interval  $(3x/4, x - 8)$  contains at least one prime.*

(iv) *For every real  $x > 27$ , the interval  $(x/2, x - 8)$  contains at least two primes.*

*Proof.* (i) For  $x < 72$  the assertion is readily verified. Suppose that  $x \geq 72$ . There exists  $\alpha \in [0, 3)$  such that  $x/3 + \alpha = 3a$  for an integer  $a > 1$ . By [13], the interval  $(3a, 4a)$  contains a prime. It remains to show that  $4a \leq x/2$ . We have  $4a = 4(x/3 + \alpha)/3 < 4x/9 + 4 = x/2 - (x/18 - 4) \leq x/2$ , since  $x/18 - 4 \geq 0$ . Hence, (i) holds.

Items (i)–(iv) can be proved in a similar manner, except that in (ii) we should use a stronger result that, for every natural  $n \geq 119$ , the interval  $[n, 1.073n]$  contains at least one prime, see [15].

$\blacktriangle$

**Lemma 7** (i) *For every natural  $n \geq 5$  there exists a decomposition  $n = n_1 + \dots + n_k$ , where  $n_1, \dots, n_k$  are pairwise coprime natural numbers at most one of which is equal to 1, such that the following property holds: for every  $1 \leq j \leq n$ , there is a decomposition  $j = j_1 + \dots + j_{k'}$  with  $k' \leq k$  and an injection  $\eta : \{j_1, \dots, j_{k'}\} \rightarrow \{n_1, \dots, n_k\}$  satisfying, for all  $i = 1, \dots, k'$ , the conditions*

(a)  $j_i \leq \eta(j_i)$ ;

(b) if  $\eta(j_i) > 1$  then  $\gcd(j_i, \eta(j_i)) > 1$ .

(ii) For every natural  $n \geq 5$  and  $1 \leq j \leq n$  such that  $(n, j) \notin \{(6, 3), (8, 3), (8, 5)\}$ , there exist a decomposition  $n = n_1 + \dots + n_k$ , where  $n_1, \dots, n_k$  are pairwise coprime natural numbers distinct from 2, 3 at most one of which is equal to 1, and a decomposition  $j = j_1 + \dots + j_{k'}$  having the same properties as in (i) and satisfying the additional requirement that  $\gcd(j_i, \eta(j_i)) \neq 3$  whenever  $\eta(j_i) = 6$ , where  $i = 1, \dots, k'$ .

*Proof.* (i) For a natural  $m > 1$ , we denote by  $\varkappa(m)$  the largest prime divisor of  $m$ .

We will show that a stronger fact holds: there exists a required decomposition  $n = n_1 + \dots + n_k$  with the additional property that

$$\varkappa(n_1 \dots n_k) \leq (n + 1)/2. \quad (6)$$

We proceed by induction on  $n$ . Suppose that  $n \leq 20$ .

If  $n = 5$  then  $n = 1 + 4$  is the required decomposition. Indeed, for  $j = 1, 2, 4$ , we may set  $k' = 1$  and  $j_1 = j$ , while, for  $j = 3$  or  $5$ , we take  $k' = 2$  and  $j = 1 + 2$  or  $j = 1 + 4$ , respectively. If  $n = 6$  then we decompose  $n = 1 + 2 + 3$ . For all  $j$ , the corresponding decomposition  $j = j_1 + \dots + j_{k'}$  is obvious. If  $n = 7$ , we set  $n = 1 + 6$ . For  $j = 1, 2, 3, 6$ , we set  $k' = 1$  and, for  $j = 4, 5, 7$ , we set  $k' = 2$  and  $j = 1 + 3, 1 + 4$ , and  $1 + 6$ , respectively. If  $n = 9$ , we set  $n = 1 + 8$ . For  $j = 1$  or  $j$  even, we set  $k' = 1$  and, for  $j > 1$  odd, we set  $k' = 2$  and  $j_1 = 1, j_2 = j - 1$ .

In all the above cases  $n = 5, 6, 7, 9$ , the injection  $\eta$  is straightforward and the property (6) holds.

Now, for  $n = 8, 10, 11, \dots, 20$  we define recursively  $n = [n - r] + r$  for the respective values  $r = 3, 5, 5, 5, 7, 7, \dots, 7, 5, 3$ , where  $[n - r]$  denotes the decomposition for  $n - r$  already defined. It is directly verified that all  $n_i$  are pairwise coprime, at most one of them is 1, and that (6) holds. If  $j \leq n - r$  then the decomposition  $j = j_1 + \dots + j_{k'}$  is defined as for  $n - r$  with the same embedding  $\eta$ , while if  $j > n - r$  then we set  $j = [j - r] + r$  and extend  $\eta$  by setting  $\eta(r) = r$ . (Note that, for  $n = 13$  and  $j = 7$ , the decomposition  $[j - r]$  is considered empty.)

Suppose that  $n \geq 21$ . By Lemma 6(i), there exists a prime  $r$  such that  $(n+1)/3 < r \leq (n+1)/2$ . Since  $n - r \geq (n - 1)/2 \geq 5$ , by induction there exists a decomposition  $n - r = n_1 + \dots + n_{k_0}$  satisfying the hypothesis and, additionally, such that  $\varkappa(n_1 \dots n_{k_0}) \leq (n - r + 1)/2$ . We show that  $n = n_1 + \dots + n_{k_0} + r$  is the required decomposition. Since  $r > (n - r + 1)/2$ , it follows that each prime divisor of each  $n_i$  is less than  $r$ ; in particular, the numbers  $n_1, \dots, n_{k_0}, r$  are pairwise coprime, at most one of them is 1, and  $\varkappa(n_1 \dots n_{k_0} r) = r \leq (n + 1)/2$ .

Now let  $1 \leq j \leq n$ . As above, if  $j \leq n - r$  then the decomposition  $j = j_1 + \dots + j_{k'}$  is defined by induction with the same embedding  $\eta$ . Suppose that  $j \geq n - r + 1$ . We have  $n - r + 1 \geq r$ . If  $j = r$  then we take this equality for a (trivial) decomposition of  $j$  and set  $\eta(r) = r$ ; otherwise,  $j > r$ , i.e.  $1 \leq j - r \leq n - r$ , and we set  $j = [j - r] + r$ , where the decomposition  $[j - r]$  and the embedding  $\eta$  on the components of  $[j - r]$  are defined by induction, and set  $\eta(r) = r$ . From the construction it is clear that all the requirements on  $\eta$  are satisfied, which completes the proof of (i).

We now prove item (ii). In this case, we will find the needed decompositions for  $n$  and  $j$  such that  $\eta(j_i) = n_i$  for all  $i = 1, \dots, k'$  (we may fix the order of the summands  $n_i$ , because  $j$  is now fixed.)

(a) First, we assume that either  $j = 2, 3, n - 2, n - 3$ , or  $(n, j) \in \{(8, 4), (16, 6), (16, 10)\}$ . Then the decompositions for  $n$  and  $j$  are shown in Table 1 in the columns labeled  $[n]$  and  $[j]$ , respectively. Note that, in each case, due to the restrictions on  $n$  and  $j$  the components  $n_i$  in  $n = n_1 + \dots + n_k$  are distinct from 2, 3, and  $(n_i, j_i) \neq 3$  whenever  $n_i = 6$ . All the remaining requirements are readily verified.

Table 1: A decomposition for  $j = 2, 3, n - 2, n - 3$  or  $(n, j) \in \{(8, 4), (16, 6), (16, 10)\}$

$(n, j)$	restrictions on $n$	$k$	$[n]$	$k'$	$[j]$
$(n, 2)$	$n \equiv 1 \pmod{2}$	2	$(n - 1) + 1$	1	2
	$n \equiv 0 \pmod{2}$	1	$n$	1	2
$(n, n - 2)$	$n \equiv 1 \pmod{2}$	2	$1 + (n - 1)$	2	$1 + (n - 3)$
	$n \equiv 0 \pmod{2}$	1	$n$	1	$n - 2$
$(n, 3)$	$n \equiv 1 \pmod{2}$	2	$1 + (n - 1)$	2	$1 + 2$
	$n \equiv 0 \pmod{6}$	1	$n$	1	3
	$n \equiv 2 \pmod{6}$	3	$1 + 4 + (n - 5)$	2	$1 + 2$
	$n \equiv 4 \pmod{6}$	2	$(n - 1) + 1$	1	3
$(n, n - 3)$	$n \equiv 1 \pmod{2}$	2	$(n - 1) + 1$	1	$n - 3$
	$n \equiv 0 \pmod{6}$	1	$n$	1	$n - 3$
	$n \equiv 2 \pmod{6}$	3	$4 + (n - 5) + 1$	2	$2 + (n - 5)$
	$n \equiv 4 \pmod{6}$	2	$1 + (n - 1)$	2	$1 + (n - 4)$
$(8, 4), (16, 6), (16, 10)$	—	1	$n$	1	$j$

(b) We may now assume that  $j \neq 2, 3, n - 2, n - 3$  and  $(n, j) \notin \{(8, 4), (16, 6), (16, 10)\}$ . We show by induction on  $n$  that in this case a stronger fact holds: there are needed decompositions  $n = n_1 + \dots + n_k$  and  $j = j_1 + \dots + j_{k'}$  with the additional requirement that  $j_i = n_i$  for all  $i = 1, \dots, k'$ .

Observe that we may also assume that  $j \leq n/2$ . (Otherwise, we take  $n - j$  instead of  $j$  and decompose  $n = n_1 + \dots + n_k$  and  $n - j = n_1 + \dots + n_{k'}$ . Then  $j = n_{k'+1} + \dots + n_k$  is the required decomposition for  $j$ , while  $n$  retains the same decompositions with the appropriate permutation of the summands.) We consider three subcases.

(b.1) Induction base. If  $n \leq 112$  then it can be directly verified that, for each admissible pair  $(n, j)$ , the required decompositions for  $n$  and  $j$  have one of the forms

- 1)  $n = (j) + (n - j), \quad j = (j);$
- 2)  $n = (1) + (j - 1) + (n - j), \quad j = (1) + (j - 1);$
- 3)  $n = (j) + (1) + (n - j - 1), \quad j = (j);$
- 4)  $n = [j] + [n - j], \quad j = [j];$

where in 1) — 3) a summand in parentheses denotes a single component of the decomposition, while in 4) a summand in brackets is decomposed as shown in Table 2. For example, if  $(n, j) = (21, 7)$  then  $\gcd(j, n - j - 1) = \gcd(7, 13) = 1$  and so the decompositions in 3) satisfy the requirements.

(b.2) Suppose that  $n \geq 113$  and  $j \leq 2n/5$ . Then  $n - j \geq 3n/5 > 57$  and by Lemma 6(ii) there is a prime  $r$  such that

$$2(n - j)/3 < r \leq n - j - 16. \quad (7)$$

Clearly,  $r \neq 2, 3$ . Moreover, we have

$$j \leq 2(n - j)/3 < r, \quad (8)$$

Table 2: An exceptional decomposition for admissible pairs  $(n, j)$ , with  $2j \leq n \leq 112$ 

$(n, j)$	$[n - j]$	$[j]$	$(n, j)$	$[n - j]$	$[j]$	$(n, j)$	$[n - j]$	$[j]$
(21, 6)	4 + 11	1 + 5	(76, 36)	40	7 + 29	(99, 22)	77	5 + 17
(25, 10)	4 + 11	1 + 9	(78, 22)	56	5 + 17	(99, 36)	63	5 + 31
(34, 12)	22	5 + 7	(81, 6)	4 + 71	1 + 5	(100, 12)	88	5 + 7
(36, 15)	21	4 + 11	(81, 15)	7 + 59	15	(100, 22)	78	5 + 17
(45, 12)	33	5 + 7	(81, 36)	45	7 + 29	(100, 45)	55	4 + 41
(46, 6)	11 + 29	6	(85, 10)	4 + 71	1 + 9	(105, 14)	91	5 + 9
(46, 10)	7 + 29	10	(85, 15)	11 + 59	15	(105, 39)	5 + 61	39
(49, 21)	5 + 23	21	(85, 34)	51	5 + 29	(105, 40)	65	7 + 33
(51, 6)	4 + 41	1 + 5	(85, 35)	9 + 41	35	(106, 6)	11 + 89	6
(51, 15)	7 + 29	15	(85, 40)	45	11 + 29	(106, 10)	7 + 89	10
(52, 18)	34	5 + 13	(88, 30)	58	7 + 23	(106, 28)	78	5 + 23
(55, 10)	4 + 41	1 + 9	(91, 21)	11 + 59	21	(106, 36)	70	13 + 23
(55, 15)	11 + 29	15	(91, 26)	65	7 + 19	(106, 40)	66	17 + 23
(55, 22)	33	5 + 17	(91, 28)	63	5 + 23	(106, 50)	56	9 + 41
(57, 21)	5 + 31	21	(91, 35)	9 + 47	35	(111, 6)	4 + 101	1 + 5
(64, 28)	36	5 + 23	(91, 39)	5 + 47	39	(111, 12)	99	5 + 7
(66, 26)	40	7 + 19	(92, 14)	5 + 73	14	(111, 15)	7 + 89	15
(69, 18)	51	5 + 13	(93, 24)	69	5 + 19	(111, 33)	5 + 73	33
(70, 24)	46	5 + 19	(96, 20)	76	7 + 13	(111, 36)	75	7 + 29
(76, 6)	11 + 59	6	(99, 21)	5 + 73	21	(111, 45)	7 + 59	45
(76, 10)	7 + 59	10						

and hence

$$(n - j)/2 < 2(n - j)/3 < r. \quad (9)$$

Now the pair  $(n - r, j)$  satisfies the induction hypothesis. Indeed, by (7) we have  $j \neq 2, 3, n - r - 2, n - r - 3$ , and  $n - r \geq j + 16 > 16$ . Hence,  $(n - r, j)$  is an admissible pair and by induction we have  $n - r = n_1 + \dots + n_k$  and  $j = n_1 + \dots + n_{k'}$ , where  $k' \leq k$  and  $n_i$ 's are pairwise coprime, distinct from 2, 3, and at most one of them being 1. Since  $r > j$  by (8), and  $r > n - r - j$  by (9), it follows that  $r$  is greater than, hence coprime with, all  $n_i$ 's. Thus  $n = n_1 + \dots + n_k + r$  and  $j = n_1 + \dots + n_{k'}$  are the required decompositions for  $n$  and  $j$ .

(b.3) Suppose that  $n \geq 113$  and  $j > 2n/5$ . Then  $j > 45$  and by Lemma 6(iii) there is a prime  $s$  such that

$$3j/4 < s < j - 8. \quad (10)$$

Since  $(n - j)/2 < 3j/4$ , we have

$$(n - j)/2 < s. \quad (11)$$

Due to  $j \leq n/2$  we also have  $(n - j)/2 \geq n/4 > 27$  and so Lemma 6(iv) implies that there is a prime  $r$  distinct from  $s$  such that

$$(n - j)/2 < r < n - j - 8. \quad (12)$$

Consider the pair  $(n - s - r, j - s)$ . By (12) and (10), we have  $j - s > 8 > 2, 3$ ;  $n - j - r > 8 > 2, 3$ ; and  $n - s - r = (n - j - r) + (j - s) > 8 + 8 = 16$ . Thus  $(n - s - r, j - s)$  is an admissible pair and by induction we have  $n - s - r = n_1 + \dots + n_k$  and  $j - s = n_1 + \dots + n_{k'}$ . By (11) and (12), we have  $s, r > (n - j)/2 \geq j/2$ . Thus  $s, r$  are distinct from, hence coprime with, all  $n_i$ 's. Therefore,  $n = s + n_1 + \dots + n_k + r$  and  $j = s + n_1 + \dots + n_{k'}$  are the required decompositions. This completes the proof of the lemma.  $\blacktriangle$

We emphasize that the difference of case (ii) from case (i) of Lemma 7 is not only in the requirement that  $n_i \neq 2, 3$  but also in that the decomposition for  $n$  depends on the number  $j$ .

Let  $r$  be a prime,  $G$  a finite group, and  $g \in G$ . We say that  $g$  is an element of  $r$ -maximal order if  $r|g| \notin \omega(G)$ . Examples of  $r$ -maximal orders for the groups  $\mathrm{SL}_n^\varepsilon(q)$  are given in Lemma 5(ii).

**Lemma 8** *Let  $S = \mathrm{SL}_n^\varepsilon(q)$ , with  $q = p^m$ .*

(i) *Let  $n \geq 5$  and  $q > 3$ . Then  $S$  contains a semisimple element  $g$  of  $p$ -maximal order such that  $\langle g \rangle \cap Z(S) = 1$  and, for every  $0 \leq j \leq n$ , the product of some  $j$  distinct characteristic values of  $g$  (in the natural  $n$ -dimensional representation) equals 1.*

(ii) *Let  $n \geq 4$ ,  $0 \leq j \leq n$ , and  $(\varepsilon, n, q) \neq (-, 4, 2)$ . Then  $S$  contains a semisimple element  $g$  of  $p$ -maximal order such that  $\langle g \rangle \cap Z(S) = 1$  and the product of some  $j$  distinct characteristic values of  $g$  (in the natural  $n$ -dimensional representation) equals 1.*

*Proof.* (i) Let  $n = n_1 + \dots + n_k$  be the decomposition whose existence is stated in Lemma 7(i). Then  $S$  includes a naturally embedded subgroup isomorphic to  $\mathrm{SL}_{n_1}^\varepsilon(q) \times \dots \times \mathrm{SL}_{n_k}^\varepsilon(q)$ . By Lemma 3(iv) and in view of the restriction  $q > 3$ , we may choose an element  $g_i \in \mathrm{SL}_{n_i}^\varepsilon(q)$  of order

$$r_i = \begin{cases} 1, & n_i = 1; \\ q_{[\varepsilon n_i]}^*, & n_i > 1. \end{cases} \quad (13)$$

Set  $g = g_1 \dots g_k \in S$  (so that  $g$  is the direct sum of diagonal blocks  $g_i$ ). By the coprimality of  $n_1, \dots, n_k$ , we have  $|g| = r_1 \dots r_k$ , and hence  $|g|$  is  $p$ -maximal by Lemma 5. Observe also that by Lemma 3(ii) either  $|g|$  is coprime with  $q - \varepsilon 1$ , or  $q = 2^l \pm 1$  and there is  $1 \leq i_0 \leq k$  such that  $n_{i_0} = 2$ . However, in the latter case, we must have  $k \geq 2$ , since  $n \geq 5$ . These remarks imply that  $\langle g \rangle \cap Z(S) = 1$  by the construction of  $g$ .

Clearly, the set of characteristic values for  $g$  is the union of those for  $g_i$  which have the form

$$\{\theta_i, \theta_i^{\varepsilon q}, \theta_i^{(\varepsilon q)^2}, \dots, \theta_i^{(\varepsilon q)^{n_i-1}}\}, \quad (14)$$

for some  $\theta_i \in F^\times$  of order  $r_i$ ,  $i = 1, \dots, k$ , where  $F$  is the algebraic closure of  $\mathbb{F}_p$ .

If  $j = 0$ , we set  $g$  to be any semisimple element of  $p$ -maximal order such that  $\langle g \rangle \cap Z(S) = 1$ . Let  $1 \leq j \leq n$  and  $j = j_1 + \dots + j_{k'}$  as stated in Lemma 7(i). Without loss of generality (renumbering, if necessary, the summands in  $n = n_1 + \dots + n_k$ ) we may assume that  $\eta(j_i) = n_i$ ,  $i = 1, \dots, k'$ , where  $\eta$  is defined in Lemma 7(i). It is sufficient to show that the product of some distinct  $j_i$  values in (14) equals 1. We may assume that  $n_i > 1$  (otherwise,  $\theta_i = 1$  and the claim holds). Then  $d_i = \gcd(j_i, n_i) > 1$  by the property (b) in Lemma 7(i). Observe that, by Lemma 3(iii), we have

$$r_i \mid \frac{(\varepsilon q)^{n_i} - 1}{(\varepsilon q)^{n_i/d_i} - 1} = 1 + x + x^2 + \dots + x^{d_i-1}, \quad x = (\varepsilon q)^{n_i/d_i}. \quad (15)$$

In particular, the set (14) is the union of  $f = n_i/d_i$  mutually disjoint subsets

$$\{\theta_i, \theta_i^x, \dots, \theta_i^{x^{d_i-1}}\}, \{\theta_i^{\varepsilon q}, \theta_i^{x(\varepsilon q)}, \dots, \theta_i^{x^{d_i-1}(\varepsilon q)}\}, \dots, \{\theta_i^{(\varepsilon q)^{f-1}}, \theta_i^{x(\varepsilon q)^{f-1}}, \dots, \theta_i^{x^{d_i-1}(\varepsilon q)^{f-1}}\},$$

in each of which the product of all elements equals 1 due to (15). Since  $j_i/d_i \leq f$  by the property (a) of Lemma 7(i), it follows that the union of arbitrary  $j_i/d_i$  of the above subsets gives the required set of  $j_i$  distinct characteristic values whose product equals 1.



(ii) As above, we may assume that  $j > 0$ . First, suppose that  $n \geq 5$  and  $(n, j) \notin \{(6, 3), (8, 3), (8, 5)\}$ . Then we decompose  $n = n_1 + \dots + n_k$  and  $j = j_1 + \dots + j_{k'}$  as stated in Lemma 7(ii). As above, there exists an element  $g = g_1 \dots g_k \in S$  of  $p$ -maximal order  $r_1 \dots r_k$ , where the  $r_i$ 's defined by (13) exist due to the restrictions  $n_i \neq 2, 3$ . We now repeat the rest of the argument of (i) to show that there are  $j$  distinct characteristic values of  $g$  whose product equals 1.

If  $(n, j) \in \{(8, 3), (8, 5)\}$  and  $(\varepsilon, q) \neq (-, 2)$  then because of (1) we may allow a summand of  $n$  to equal 3. So we decompose  $n = 5 + 3$ ,  $j = j$  (trivial decomposition). If  $(n, j, \varepsilon, q) \neq (6, 3, +, 2)$  then the divisibility (15) holds by (2) and we may repeat the above argument.

If  $n = 4$  and  $(\varepsilon, q) \neq (-, 2)$  then again 3 is a possible summand for  $n$  and so we decompose  $n = 1 + 3$  if  $j = 1$  or 3, and decompose trivially  $n = 4$  if  $j = 2$  or 4 and proceed as above.

Suppose that  $S = \mathrm{SL}_6(2)$  and  $j = 3$ . Then  $S$  contains an element  $g$  of 2-maximal order 21 whose characteristic values are  $\nu_i = \theta^{2^{i-1}}$ ,  $i = 1, \dots, 6$ , where  $\theta \in \overline{\mathbb{F}}_2^\times$  is of order 21. Observe that  $Z(S) = 1$  and the product of 3 characteristic values  $\nu_1, \nu_3, \nu_5$  of  $g$  equals  $\theta\theta^4\theta^{16} = 1$ , as required.

Finally, let  $S = \mathrm{SU}_8(2)$  and  $j = 3$  or 5. Then  $S$  contains an element  $g$  of order 45 (which is 2-maximal) and whose block-diagonal form  $g = g_1 g_2 g_3$  has three blocks of sizes 4, 3, 1 and the characteristic values  $\nu_1, \dots, \nu_8$  of  $g$  are

$$\underbrace{\theta^3, (\theta^3)^{-2}, (\theta^3)^4, (\theta^3)^{-8}}_{g_1}, \underbrace{\theta^{-5}, (\theta^{-5})^{-2}, (\theta^{-5})^4}_{g_2}, \underbrace{\theta^{30}}_{g_3}; \quad (16)$$

where  $\theta \in \overline{\mathbb{F}}_2^\times$  is of order 45. Then  $\nu_1 \nu_3 \nu_8 = \nu_2 \nu_4 \nu_5 \nu_6 \nu_7 = 1$  and so there are  $j$  characteristic values of  $g$  whose product equals 1. Since  $Z(S) = 1$ , the claim follows.  $\blacktriangle$

**Lemma 9** *If a Frobenius group  $KC$  with kernel  $K$  and cyclic complement  $C = \langle c \rangle$  of order  $n$  acts faithfully on a vector space  $V$  over a field of nonzero characteristic  $p$  coprime with the order of  $K$ , then the minimal polynomial of  $c$  on  $V$  is  $x^n - 1$ . In particular, the semidirect product  $V \rtimes C$  contains an element of order  $p \cdot n$  and  $\dim C_V(c) > 0$ .*

*Proof.* See [16, Lemma 1].  $\blacktriangle$

**Lemma 10** *A group  $H$  is recognizable by spectrum from its covers if and only if  $\omega(H) = \omega(G)$  for every split extension  $G = N \rtimes H$ , where  $N$  is an elementary abelian  $r$ -group for some  $r$  and  $H$  acts on  $N$  absolutely irreducibly.*

*Proof.* Let  $G$  be a proper cover for  $H$  of minimal order such that  $\omega(H) = \omega(G)$ . By [10, Lemma 12], we may assume that  $G = N \rtimes H$ , where  $H$  acts on the elementary abelian  $r$ -group  $N$  irreducibly. Suppose that this action is not absolutely irreducible. Let  $F$  be a finite splitting field for  $H$  of characteristic  $r$  and consider a proper submodule  $N_0$  of the reducible  $FH$ -module  $N \otimes_{\mathbb{F}_p} F$ . It is sufficient to show that  $\omega(N_0 \rtimes H) = \omega(H)$ . Suppose to the contrary that  $n_0 h \in N_0 \rtimes H$  is an element of order not belonging to  $\omega(H)$ . Then the element  $1 + h + h^2 + \dots + h^{|h|-1}$  considered as a linear transformation of  $N_0$  is nonzero. But then it is also nonzero as a linear transformation of  $N$  and hence  $G$  contains an element  $nh$  of order  $|n_0 h|$ , a contradiction.  $\blacktriangle$

**Lemma 11** *Let  $r$  be a prime and let  $L = \mathrm{L}_n^\varepsilon(q)$  be a simple group, where  $q = p^m$  and  $\varepsilon \in \{+, -\}$ . Then  $\omega(\mathbb{Z}_r \times L) \not\subseteq \omega(L)$ .*

*Proof.* Denote by  $a_1$  and  $a_2$  the numbers in (3). By Lemma 5(i), there is  $i = 1, 2$  such that  $r \nmid a_i$  and  $ra_i \notin \omega(L)$ . Since  $ra_i \in \omega(\mathbb{Z}_r \times L)$ , the claim follows.  $\blacktriangle$

**Lemma 12** *Let  $L = L_n(q)$  be a simple linear group, where  $q = p^m$ . Then  $L$  is recognizable by spectrum from its covers if and only if  $\omega(L) = \omega(G)$  for every split extension  $G = N \rtimes L$ , where  $N$  is an elementary abelian  $p$ -group and  $L$  acts on  $N$  faithfully and absolutely irreducibly.*

*Proof.* By Lemma 10, we may assume that  $G = N \rtimes L$  where  $N$  is an elementary abelian  $r$ -group for some  $r$  and  $L$  acts on  $N$  absolutely irreducibly. By Lemma 11,  $L$  acts faithfully. The image in  $L$  of the parabolic subgroup of  $SL_n(q)$  of the shape  $q^{n-1} : GL_{n-1}(q)$  contains by [3, Lemma 5] a Frobenius subgroup  $KC$  with elementary abelian kernel  $K$  of order  $q^{n-1}$  and cyclic complement  $C$  of order  $a = (q^{n-1} - 1)/d$ , where  $d = \gcd(n, q - 1)$ . If  $r \neq p$  then, by Lemma 9, we have  $ra \in \omega(G)$ . However,  $ra \notin \omega(L)$  by Lemma 5(i). Hence,  $r = p$ .  $\blacktriangle$

### 3 Weights of irreducible $SL_n(F)$ -modules

In this section, we recall some facts from the representation theory of algebraic groups. For details, see e. g. [12].

Let  $G = SL_n(F)$ , where  $F$  is an algebraically closed field of characteristic  $p$ . Then  $G$  is a simply connected simple algebraic group of type  $A_l$ , where  $l = n - 1$ . Denote by  $\omega_0$  the zero weight and by  $\omega_1, \dots, \omega_l$  the fundamental weights of  $G$  (with respect to a fixed maximal torus of  $G$  and a system of positive roots). Let  $\Omega = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_l$  be the weight lattice and  $\Delta$  the root system of  $G$  with the set  $\alpha_1, \dots, \alpha_l$  of simple roots. Also, let  $\Omega_0 = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_l$  be the set of *radical weights* and  $\Omega^+ = \{a_1\omega_1 + \dots + a_l\omega_l \in \Omega \mid a_1 \geq 0, \dots, a_l \geq 0\}$  be the set of *dominant weights*. The weights in the set  $\Omega_k^+ = \{a_1\omega_1 + \dots + a_l\omega_l \in \Omega \mid 0 \leq a_1 < k, \dots, 0 \leq a_l < k\}$  are called *k-restricted*, where  $k$  is usually a power of  $p$ .

For an irreducible (rational, finite dimensional)  $G$ -module  $L$ , denote by  $\Omega(L)$  the set of weights of  $L$  and by  $\lambda(L)$  the highest weight of  $L$ . It is known that  $\lambda(L) \in \Omega^+$  and each dominant weight is the highest weight of some irreducible module  $L$ . The irreducible  $G$ -module of highest weight  $\lambda$  is customarily denoted by  $L(\lambda)$ . Obviously,  $\Omega(L(\omega_0)) = \{\omega_0\}$ . The module  $L$  is called *p-restricted* if  $\lambda(L) \in \Omega_p^+$ . The modules  $L(\omega_i)$ ,  $i = 1, \dots, l$  are called the *microweight modules*. The structure of the microweight modules is well known and described in the following lemma (see, e.g. [12, II.2.15]):

**Lemma 13** *Let  $G = SL_n(F)$  and let  $V = F^n$  be the natural  $G$ -module with the canonical basis  $e_1, \dots, e_n$ . Choose the diagonal subgroup  $H$  for a fixed maximal torus of  $G$ . Then  $e_i$  is an eigenvector for  $H$  with the corresponding weight  $\varepsilon_i$ . Choose a system of positive roots  $\{\varepsilon_i - \varepsilon_j \mid 1 \leq i < j \leq n\}$ . Then, for  $1 \leq k < n$ , we have  $\omega_k = \varepsilon_1 + \dots + \varepsilon_k$  and the microweight module  $L(\omega_k)$  is isomorphic to the  $k$ -th exterior power  $\wedge^k V$  and has the set of weights*

$$\Omega(L(\omega_k)) = \{\varepsilon_{i_1} + \varepsilon_{i_2} + \dots + \varepsilon_{i_k} \mid 1 \leq i_1 < i_2 < \dots < i_k \leq n\}.$$

The following assertion is a refinement of [9, Proposition 2.3] for groups of type  $A_l$ .

**Lemma 14** *Let  $G = SL_n(F)$  and let  $L$  be an irreducible  $p$ -restricted  $G$ -module. Write  $\lambda(L) = a_1\omega_1 + \dots + a_l\omega_l$ . Suppose that  $i \in \{0, 1, \dots, l\}$  is the uniquely defined integer such that*

$$a_1 + 2a_2 + \dots + la_l \equiv i \pmod{l+1}. \quad (17)$$

*Then  $\Omega(L(\omega_i)) \subseteq \Omega(L)$ .*

*Proof.* By [12, Proposition II.2.4],  $\Omega(L)$  lies in a single coset of  $\Omega : \Omega_0$  and, by [9, Proposition 2.3],  $\Omega(L)$  contains  $\omega_0$  if  $\lambda(L)$  is radical, and includes  $\Omega(L(\omega_i))$  for some  $i = 1, \dots, l$ , otherwise. In the latter case, the index  $i$  is uniquely defined, since the weights  $\omega_0, \omega_1, \dots, \omega_l$  form a transversal of  $\Omega : \Omega_0$  by [11, VIII, §7.3, Proposition 8].

Therefore, it remains to observe that an arbitrary weight  $\lambda = a_1\omega_1 + \dots + a_l\omega_l \in \Omega$  lies in the coset  $\omega_i + \Omega_0$  if and only if (17) holds. Indeed, if  $\lambda = \alpha_i$  is a simple root then  $(a_1, \dots, a_l)$  is the  $i$ th row of the Cartan matrix of type  $A_l$  and (17) is directly verified. By the above, every weight  $\lambda$  is in  $\omega_i + \Omega_0$  for some  $i$  and adding or subtracting positive roots from  $\lambda$  preserves the relation (17) and the coset  $\omega_i + \Omega_0$ . The claim follows from these remarks.  $\blacktriangle$

## 4 Proofs of the main results

We first give a proof of Theorem 1.

*Proof.* By Lemma 10, we may assume that  $W$  is absolutely irreducible as a module for  $L$ . Moreover, by [14, Theorem 43], we may assume that  $W$  is a restriction to  $S = \mathrm{SL}_n^\varepsilon(q)$  of an irreducible module  $L(\lambda)$  for  $G = \mathrm{SL}_n(F)$ , where  $\lambda \in \Omega_q^+$ , and  $F = \overline{\mathbb{F}}_p$ . Set  $l = n - 1$ .

(a) We first consider the case where  $n \geq 5$  and  $q > 3$ . It is sufficient to show that there is a semisimple element  $g \in S$  of  $p$ -maximal order such that  $\langle g \rangle \cap Z(S) = 1$  which centralizes a nonzero vector  $w \in W$ . Indeed, if this is the case then the element  $w\bar{g} \in W \setminus L$  has order  $p|g| \notin \omega(L)$ , due to  $\omega(L) \subseteq \omega(S)$ , where  $\bar{g}$  is the image of  $g$  in  $L$ .

We choose for a fixed maximal torus of  $G$  the diagonal subgroup  $H$ . Write

$$\lambda = \lambda_0 + p\lambda_1 + \dots + p^{m-1}\lambda_{m-1}, \quad \lambda_i \in \Omega_p^+.$$

By the Steinberg Tensor Product theorem [14, Theorem 41], we have

$$L(\lambda) \cong L(\lambda_0) \otimes L(\lambda_1)^\rho \otimes \dots \otimes L(\lambda_{m-1})^{\rho^{m-1}}, \quad (18)$$

where  $\rho$  denotes the twisting by the Frobenius map corresponding to the automorphism  $x \mapsto x^p$  of  $F$ . By Lemma 14, for each  $i = 0, \dots, m-1$ , there exists  $k_i \in \{0, \dots, l\}$  such that  $\Omega(L(\omega_{k_i})) \subseteq \Omega(L(\lambda_i))$ . In particular, the set  $\Omega(L(\lambda))$  contains all possible weights of the form

$$\mu_0 + p\mu_1 + \dots + p^{m-1}\mu_{m-1}, \quad \mu_i \in \Omega(L(\omega_{k_i})). \quad (19)$$

By Lemma 13,  $\mu_i$  can be an arbitrary sum of  $k_i$  distinct weights in  $\{\varepsilon_1, \dots, \varepsilon_n\}$ .

Let  $g \in S$  be the semisimple element whose existence is stated in Lemma 8(i). Then there is  $a \in G$  such that  $h = {}^a g \in H$ . By Lemma 8(i), there are  $k_i$  distinct characteristic values of  $g$  whose product equals 1 and we define  $\mu_i$  to be the sum of the corresponding  $k_i$  weights  $\varepsilon_j$  so that  $\mu_i(h) = 1$  for all  $i = 0, \dots, m-1$ . Denote by  $\mu$  the sum (19) with  $\mu_i$  just defined. Then we have  $\mu \in \Omega(L(\lambda))$  and

$$\mu(h) = \mu_0(h)\mu_1(h)^p \dots \mu_{m-1}(h)^{p^{m-1}} = 1.$$

Let  $w_0 \in W$  be a weight vector for  $G$  of weight  $\mu$  so that  $w_0 h = \mu(h)w_0 = w_0$ . Set  $w = w_0 a$ . Then

$$wg = w_0 a g = w_0 h a = w_0 a = w.$$

Thus  $g$  is the required semisimple element of  $S$ .

(b) We now suppose that  $n \geq 4$ ,  $q$  is prime, and  $(\varepsilon, n, q) \neq (-, 4, 2)$ . In this case,  $\lambda \in \Omega_q^+ = \Omega_p^+$ . By Lemma 14, there exists  $j \in \{0, \dots, l\}$  such that  $\Omega(L(\omega_j)) \subseteq \Omega(L(\lambda))$ . Hence, by Lemma 13,  $\Omega(L(\lambda))$  contains the sum of arbitrary  $j$  distinct weights in  $\{\varepsilon_1, \dots, \varepsilon_n\}$ . Now, we choose by Lemma 8(ii) a semisimple element  $g \in S$  of  $p$ -maximal order such that  $\langle g \rangle \cap Z(S) = 1$  and the product of some  $j$  distinct characteristic values of  $g$  equals 1. There is  $a \in G$  such that  $h = {}^a g \in H$  and so the product of some  $j$  characteristic values of  $h$  equals 1 as well. We set  $\mu$  equal to the sum of the corresponding  $j$  weights  $\{\varepsilon_1, \dots, \varepsilon_n\}$  so that  $\mu(h) = 1$ . (Then  $\mu \in \Omega(L(\lambda))$  by the above.) If now  $w_0 \in W$  is a weight vector for  $G$  then, as in case (a),  $wg = w$ , where  $w = w_0 a$  and so  $g$  is as required.

We emphasize that, in this cases, the principal difference from case (a) is that the module  $W$  is  $p$ -restricted and that the choice of  $g$  depends on  $W$ .

(c) Finally, let  $n = 4$  and let  $q$  be even. By Lemma 6 in [4],  $L$  contains a Frobenius subgroup  $KC$  with kernel  $K$  of order  $q_{[4]}$  and cyclic complement  $C$  of order 4. By Lemma 11,  $KC$  acts faithfully on  $W$  and hence Lemma 9 implies that  $2|C| \in \omega(W \rtimes L)$ . However,  $2|C| = 8 \notin \omega(L)$  by Lemma 4. This completes the proof of the theorem.  $\blacktriangle$

Corollary 1 is now a direct consequence of Lemma 12 and Theorem 1.

*Acknowledgement.* The author is thankful to D. O. Revin for reading the manuscript of the paper and making a number of valuable remarks.

## References

- [1] Unsolved problems in group theory, *The Kourovka notebook*, 14th ed., Sobolev Inst. Mat. (Novosibirsk), 1999.
- [2] A. V. Zavarnitsine, Weights of the irreducible  $\mathrm{SL}_3(q)$ -modules in defining characteristic. (Russian) *Sibirsk. Mat. Zh.*, **45**, N 2 (2004), 319–328. English translation in *Sib. Math. J.*, **45**, N 2 (2004), 261–268
- [3] A. V. Vasil’ev and M. A. Grechkoseeva, On Recognition by Spectrum of Finite Simple Linear Groups over Fields of Characteristic 2. (Russian) *Sibirsk. Mat. Zh.*, **46**, N 4 (2005), 749–758. English translation in *Sib. Math. J.*, **46**, N 4 (2005), 593–600.
- [4] V. D. Mazurov, A. V. Zavarnitsine, On element orders in coverings of the simple groups  $L_n(q)$  and  $U_n(q)$ , *Proceedings of the Steklov Institute of Mathematics*, Suppl. 1 (2007), 145–154.
- [5] R. Brandl, W. Shi, The characterization of  $\mathrm{PSL}_2(q)$  by its element orders, *J. Algebra*, **163** (1994), N 1, 109–114.
- [6] V. D. Mazurov, A. V. Zavarnitsine, Element orders in coverings of symmetric and alternating groups. (Russian) *Algebra i Logika*, **38**, N 3 (1999), 296–315. Translation in *Algebra and Logic*, **38**, N 3 (1999), 159–170.
- [7] R. W. Carter, Centralizers of semisimple elements in the finite classical group, *Proc. London Math. Soc.* (3), **42**, N 1 (1981), 1–41
- [8] D. M. Testerman,  $A_1$ -type overgroups of elements of order  $p$  in semisimple algebraic groups and the associated finite groups, *J. Algebra*, **177**, N 1, (1995), 34–76.

- [9] I. D. Suprunenko, A. E. Zalesskii, Fixed vectors for elements in modules for algebraic groups, *Internat. J. Algebra Comput.*, **17**, N 5–6 (2007), 1249–1261.
- [10] A. V. Zavarnitsine, Recognition of the simple groups  $L_3(q)$  by element orders. *J. Group Theory*, **7**, N 1, (2004), 81–97.
- [11] N. Bourbaki, Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées. Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, (1975).
- [12] J. C. Jantzen, Representations of algebraic groups. Second edition. Mathematical Surveys and Monographs, 107. American Mathematical Society, Providence, RI, 2003.
- [13] D. Hanson, On a theorem of Sylvester and Schur, *Canad. Math. Bull.* **16** (1973), 195–199.
- [14] R. Steinberg, Lectures on Chevalley groups. (Russian) Biblioteka sbornika "matematika", Moscow: Verlag "Mir", (1975).
- [15] H. Rohrbach, J. Weis, Zum finiten Fall des Bertrandschen Postulates. *J. Reine Angew. Math.*, 214/215 (1964), 432–440.
- [16] V. D. Mazurov, On the set of orders of elements of a finite group. (Russian) *Algebra i Logika*, **33**, N 1 (1994), 81–89. Translation in *Algebra and Logic* **33**, N 1 (1994), 49–55.